Computing the Communication Complexity of Quantum Channels

A. Montina, M. Pfaffhauser, S. Wolf
Facoltà di Informatica, Università della Svizzera Italiana, Via G. Buffi 13, 6900 Lugano, Switzerland
(Dated: January 21, 2013)

The communication complexity of a quantum channel is the minimal amount of classical communication required for classically simulating the process of preparation, transmission through the channel, and subsequent measurement of a quantum state. At present, only little is known about this quantity. In this paper, we present a procedure for systematically evaluating the communication complexity of channels in any general probabilistic theory, in particular quantum theory. The procedure is constructive and provides the most efficient classical protocols. We illustrate this procedure by evaluating the communication complexity of a noiseless quantum channel with some finite sets of quantum states and measurements.

arXiv:1301.4441v1 [quant-ph] 18 Jan 2013

Quantum communication has proved to be much more powerful than its classical counterpart. Indeed, quantum channels can provide an exponential saving of communication resources in some distributed computing problems [1], where the task is to evaluate a function of data held by two or more parties. A natural measure of power of quantum communication is provided by the communication complexity of a quantum channel, which is defined as the minimal amount of classical communication required for classically simulating the process of preparation, transmission through the channel, and subsequent measurement of a quantum state. Indeed, it is clear that a quantum channel cannot replace an amount of classical communication greater than its communication complexity. Thus, this quantity sets an ultimate limit to the power of quantum communication in a two-party scenario in terms of classical resources.

At present, only little is known about the communication complexity of quantum channels. Toner and Bacon proved that two classical bits are sufficient to simulate the communication of a single qubit [2]. In the case of parallel simulations, the communication can be compressed so that the asymptotic cost per simulation is about 1.28 bits [3]. Simulating the communication of n qubits requires an amount of classical communication greater than or equal to $2^n - 1$ bits [4]. However, no upper bound is known.

In this paper, we present a general procedure for systematically evaluating the communication complexity of channels in any general probabilistic theory, in particular quantum theory. The procedure relies on the reverse Shannon theorem [5] and a strategy discussed in Refs. [3, 6]. We illustrate this procedure by evaluating the communication complexity of a noiseless quantum channel with some finite sets of quantum states and measurements.

A protocol simulating a quantum channel actually simulates a process of preparation, transmission through the channel and subsequent measurement of a quantum state. For the sake of simplicity, we will focus on noiseless quantum channels, but the following discussion can be easily generalized to any probabilistic theory, as pointed out later. The simulated quantum scenario is as follows. A party, say Alice, prepares n qubits in some quantum state $|\psi\rangle$. Then, she sends the qubits to another party, say Bob. Finally, Bob generates an outcome by performing a measurement $\mathcal{M} = \{\hat{E}_1, \hat{E}_2, \dots\}$, where $\hat{E}_i$ are positive semidefinite self-adjoint operators labeling events of the measurement $\mathcal{M}$. In a classical simulation, the quantum channel between Alice and Bob is replaced by classical communication. A classical protocol is as follows. Alice sets a variable, say k, according to a probability distribution $\rho(k|y,\psi)$ that depends on the quantum state $|\psi\rangle$ and, possibly, a random variable y shared with Bob. Thus, there is a mapping from the quantum state to a probability distribution of k,

$$|\psi\rangle \xrightarrow{y} \rho(k|y,\psi). \tag{1}$$

Alice sends k to Bob, who simulates a measurement $\mathcal{M}$ by generating an outcome $\hat{E}_w$ with a probability $P(w|k,y,\mathcal{M})$. The protocol exactly simulates the quantum channel if the probability of $\hat{E}_w$ given $|\psi\rangle$ is equal to the quantum probability, that is, if

$$\sum_k \int dy P(w|k,y,\mathcal{M})\rho(k|y,\psi)\rho(y) = \langle\psi|\hat{E}_w|\psi\rangle, \tag{2}$$

where $\rho(y)$ is the probability density of the random variable y. Let us denote by $\rho(k|y) \equiv \int d\psi \sum \rho(k|y,\psi)\rho(\psi)$ the marginal conditional probability of k given y. As defined in Ref. [6], the communication cost, say $\mathcal{C}$, of the classical simulation is the maximum, over the space of distributions $\rho(\psi)$, of the Shannon entropy of the distribution $\rho(k|y)$ averaged over y, that is,

$$\mathcal{C} \equiv \max_{\rho(\psi)} H(K|Y), \tag{3}$$

where $H(K|Y) \equiv -\int dy \rho(y) \sum_k \rho(k|y) \log_2 \rho(k|y)$.

This definition relies on the Shannon coding theorem, as discussed in Ref. [6]. We define the *communication complexity* (denoted by $\mathcal{C}_{min}$) of a quantum channel as the minimal amount of classical communication $\mathcal{C}$ required by an exact classical simulation of the quantum channel, given any measurement $\mathcal{M}$. Let

$\mathbf{S} \equiv \{|\psi_1\rangle, \dots, |\psi_S\rangle\}$ and $\mathbf{M} \equiv \{\mathcal{M}_1, \dots, \mathcal{M}_M\}$ be a set of S quantum states and M measurements, respectively. We define the communication complexity, say $\mathcal{C}_{min}(\mathbf{G})$, of the quantum game $(\mathbf{S}, \mathbf{M}) \equiv \mathbf{G}$ as the minimal amount of classical communication required to simulate the quantum channel with the restriction that the quantum states and the measurements are elements of $\mathbf{S}$ and $\mathbf{M}$, respectively.

Let us consider the case of R quantum channels. In a general parallel simulation, the communicated variable k is generated according to a probability distribution $\rho(k|y, \psi^1, \psi^2, \dots, \psi^R)$ depending on the whole set of R prepared quantum states $|\psi^1\rangle, \dots, |\psi^R\rangle$ (superscripts will always label channels simulated in parallel). Thus, the single-shot map (1) is replaced by

$$\{|\psi^1\rangle, \dots, |\psi^R\rangle\} \xrightarrow{y} \rho(k|y, \psi^1, \psi^2, \dots, \psi^R). \quad (4)$$

The asymptotic communication cost, say $\mathcal{C}^{asym}$, is equal to $\lim_{R\to\infty} \mathcal{C}^{par}/R$, $\mathcal{C}^{par}$ being the cost of the parallelized simulation. The definition of $\mathcal{C}^{par}$ is similar to that of $\mathcal{C}$, with the difference that the maximization is made over the space of the distributions $\rho(\psi^1, \dots, \psi^R)$. We define the asymptotic communication complexity, $\mathcal{C}_{min}^{asym}$, of a quantum channel as the minimal asymptotic communication cost required for simulating the channel. The asymptotic communication complexity of the game $\mathbf{G}$ is similarly defined.

Given a game $\mathbf{G} = (\mathbf{S}, \mathbf{M})$, let $\mathbf{w} = \{w_1, \dots, w_M\}$ be an M-dimensional array whose m-th element is one of the possible outcomes of the m-th measurement $\mathcal{M}_m \in \mathbf{M}$. We denote by $s = 1, \dots, S$ and $m = 1, \dots, M$ discrete indices labelling the elements of $\mathbf{S}$ and $\mathbf{M}$, respectively. The summation over every index in $\mathbf{w}$ but the m-th one, which is set equal to w, is concisely written as follows,

$$\sum_{w_1,\dots,w_{m-1},w_m=w,\dots,w_M} \to \sum_{\mathbf{w},w_m=w} \quad (5)$$

Definition. Given a game $\mathbf{G} = (\mathbf{S}, \mathbf{M})$, the set $\mathcal{V}(\mathbf{G})$ contains any conditional probability $\rho(\mathbf{w}|s)$ whose marginal distribution of the m-th variable is the quantum distribution of the outcome w_m given the quantum state s and the measurement m, for any s, m. In other words, the set $\mathcal{V}(\mathbf{G})$ contains any $\rho(\mathbf{w}|s)$ satisfying the constraints

$$\sum_{\mathbf{w},w_m=w} \rho(\mathbf{w}|s) = P_Q(w|s,m), \forall s, m \text{ and } w, \quad (6)$$

where $P_Q(w|s,m) \equiv \langle\psi_s|\hat{E}_{m;w}|\psi_s\rangle$ is the quantum probability of getting the w-th outcome $\hat{E}_{m;w}$ of the measurement $\mathcal{M}_m$ given the quantum state $|\psi_s\rangle$.

The set $\mathcal{V}(\mathbf{G})$ is surely non-empty. A function in $\mathcal{V}(\mathbf{G})$ is $\rho(\mathbf{w}|s) = P_Q(w_1|s,1) \times \dots \times P_Q(w_M|s,M)$, where the variables $w_1, \dots, w_M$ are uncorrelated. The definition of $\mathcal{V}(\mathbf{G})$ can be easily extended to any general probabilistic theory, where $P_Q(w|s,m)$ is replaced by different conditional probabilities. For the sake of concreteness, we will refer to the quantum case, but the following discussion does not rely on any precise form of $P_Q(w|s,m)$ and applies to more general theories.

A pivotal classical protocol for the quantum game $\mathbf{G}$ is as follows.

Master protocol. Alice generates the array $\mathbf{w}$ according to a conditional probability $\rho(\mathbf{w}|s) \in \mathcal{V}(\mathbf{G})$. Then, she sends $\mathbf{w}$ to Bob. Bob simulates the measurement $\mathcal{M}_m$ by generating the outcome w_m.

The definition of $\mathcal{V}(\mathbf{G})$ implies that this protocol exactly simulates the quantum game $\mathbf{G}$. A classical channel from a variable x_1 to x_2 is defined by the conditional probability of getting x_2 given x_1. Its capacity is the maximum of the mutual information between x_1 and x_2 over the space of probability distributions $\rho(x_1)$ [7]. Using the strategy discussed in Ref. [3] and the reverse Shannon theorem [5], it is possible to prove that a master protocol can be turned into a child protocol for parallel simulations whose asymptotic communication cost is equal to the capacity of the classical channel $\rho(\mathbf{w}|s)$.

Lemma 1. Given a conditional probability $\rho(\mathbf{w}|s) \in \mathcal{V}(\mathbf{G})$, there is a child protocol, simulating in parallel R quantum games $\mathbf{G}$, whose asymptotic communication cost per game is equal to the capacity of the channel $\rho(\mathbf{w}|s)$ as R goes to infinity.

Proof. In a simulation of R games $\mathbf{G}$ through R master protocols performed in parallel, Alice sends an array $\mathbf{w}$ to Bob for each game. This array is generated with probability $\rho(\mathbf{w}|s)$. Let $C(\mathbf{W}|S)$ be the capacity of the channel $T: s \to \mathbf{w}$. The child protocol is as follows. Instead of sending $\mathbf{w}$, Alice sends an amount of information, say $\mathcal{C}(R)$, that allows Bob to generate $\mathbf{w}$ for every game $\mathbf{G}$ according to the probability $\rho(\mathbf{w}|s)$. The reverse Shannon theorem states that this can be accomplished with a cost $\mathcal{C}(R)$ such that $\lim_{R\to\infty} \mathcal{C}(R)/R = C(\mathbf{W}|S)$, provided that the receiver and sender share some random variable. □

The first main result is the following theorem about the asymptotic communication complexity. Later on, we will consider the single-shot case.

Theorem 1. The asymptotic communication complexity of the game $\mathbf{G} = (\mathbf{S}, \mathbf{M})$ is the minimum of the capacity of the classical channels $\rho(\mathbf{w}|s)$ in the set $\mathcal{V}(\mathbf{G})$.

Theorem 1 states that the asymptotic communication complexity of the game $\mathbf{G}$ is equal to the quantity

$$\mathcal{D}(\mathbf{G}) \equiv \min_{\rho(\mathbf{w}|s)\in\mathcal{V}(\mathbf{G})} \left(\max_{\rho(s)} I(\mathbf{W}; S) \right), \quad (7)$$

where $I(\mathbf{W}; S)$ is the mutual information between the stochastic variables $\mathbf{w}$ and s.

Proof. Lemma 1 implies that $\mathcal{C}_{min}^{asym}(\mathbf{G}) \le \mathcal{D}(\mathbf{G})$. We show that $\mathcal{C}_{min}^{asym}(\mathbf{G})$ is actually equal to $\mathcal{D}(\mathbf{G})$ by proving that the asymptotic communication cost cannot be smaller than $\mathcal{D}(\mathbf{G})$. Let $\mathcal{C}_0$ be the asymptotic communication cost of a parallel simulation of the game $\mathbf{G}$. We denote by R the number of games $\mathbf{G}$ that are simulated in parallel. In the simulation, Alice sends a variable k generated with conditional probability $\rho(k|y, s^1, \dots, s^R)$, where s^i is an index labelling the quantum state of the i-th game. Bob simulates the measurements $\mathcal{M}_{m^1}, \dots, \mathcal{M}_{m^R}$ by generating the outcomes $w^1, \dots, w^R$ according to a conditional probability $P(w^1, \dots, w^R|k, y, m^1, \dots, m^R)$. Let us denote by $P^i(w^i|k, y, m^1, \dots, m^R)$ the marginal probability of the outcome of the i-th game. We introduce the conditional probabilities

$$P^i(\mathbf{w}^i|k, y) = \prod_{m^i} P^i(w^i_{m_i}|k, y, 1, \dots, m^i, \dots, 1), \quad (8)$$

where $\mathbf{w}^i \equiv \{w^i_1, \dots, w^i_M\}$. Note that we have multiplied over m^i and set the other indices equal to 1. For our purposes, any other choice of the values of the $R-1$ indices would be fine. We use $P^i(\mathbf{w}^i|k, y)$ to build the conditional probability

$$P(\mathbf{w}^1, \dots, \mathbf{w}^R|k, y) = \prod_i P^i(\mathbf{w}^i|k, y). \quad (9)$$

Finally, from this distribution and $\rho(k|y, s^1, \dots, s^R)$, we build the conditional probability

$$\rho(\mathbf{w}^1, \dots, \mathbf{w}^R|s^1, \dots, s^R) = \sum_k \int dy \rho(y) P(\mathbf{w}^1, \dots, \mathbf{w}^R|k, y) \rho(k|y, s^1, \dots, s^R). \quad (10)$$

From the data-processing inequality [7], we have that the capacity, say $C(\mathbf{W}^1, \dots, \mathbf{W}^R|S^1, \dots, S^R)$, of $\rho(\mathbf{w}^1, \dots, \mathbf{w}^R|s^1, \dots, s^R)$ is smaller than or equal to the communication cost $R\,\mathcal{C}_0 + o(R)$, that is,

$$C(\mathbf{W}^1, \dots, \mathbf{W}^R|S^1, \dots, S^R) \le R\,\mathcal{C}_0 + o(R). \quad (11)$$

By construction, we have the constraints

$$\sum_{\mathbf{w}^1, \dots, \mathbf{w}^R, w^i_m = w} \rho(\mathbf{w}^1, \dots, \mathbf{w}^R|s^1, \dots, s^R) = P_Q(w|s_i, m), \quad (12)$$

the left-hand side being the marginal distribution of the variable w^i_m (renamed w) given $s^1, \dots, s^R$. Let $\rho_0(\mathbf{w}|s)$ be the probability distribution in $\mathcal{V}(\mathbf{G})$ with minimal capacity $\mathcal{D}(\mathbf{G})$. The probability distribution

$$\rho_{min}(\mathbf{w}^1, \dots, \mathbf{w}^R|s^1, \dots, s^R) \equiv \prod_i \rho_0(\mathbf{w}^i|s^i), \quad (13)$$

is the channel satisfying constraints (12) with minimal capacity. The minimum is equal to $R\,\mathcal{D}(\mathbf{G})$. Thus,

$$R\,\mathcal{D}(\mathbf{G}) \le C(\mathbf{W}^1, \dots, \mathbf{W}^R|S^1, \dots, S^R). \quad (14)$$

From this inequality and Inequality (11) we have that

$$R\mathcal{D}(\mathbf{G}) \le R\mathcal{C}_0 + o(R). \quad (15)$$

The theorem is proved. □

Theorem 1 and Lemma 1 have their one-shot versions.

Lemma 2 (One-shot version of Lemma 1). Given a conditional probability $\rho(\mathbf{w}|s) \in \mathcal{V}(\mathbf{G})$, there is protocol simulating a quantum game $\mathbf{G}$ such that

$$C_{ch} \le \mathcal{C} \le C_{ch} + 2\log_2(C_{ch} + 1) + 2\log_2 e,$$

where $\mathcal{C}$ and C_{ch} are the communication cost of the simulation and the capacity of the channel $\rho(\mathbf{w}|s)$.

The proof is similar to that of Lemma 1 and relies on the one-shot version of the reverse Shannon theorem proved in Ref. [8].

Theorem 2 (One-shot version of Theorem 1). The communication complexity $\mathcal{C}_{min}(\mathbf{G})$ of the game $\mathbf{G}$ satisfies the inequalities

$$\mathcal{D}(\mathbf{G}) \le \mathcal{C}_{min}(\mathbf{G}) \le \mathcal{D}(\mathbf{G}) + 2\log_2[\mathcal{D}(\mathbf{G}) + 1] + 2\log_2 e,$$

where $\mathcal{D}(\mathbf{G})$ is given by Eq. (7) and it is equal to the asymptotic communication complexity of the game $\mathbf{G}$ (Theorem 1).

The first inequality is a trivial consequence of Theorem 1, as the asymptotic communication complexity cannot be larger than the communication complexity. The second inequality comes from Lemma 2.

Thus, the communication complexity of a quantum channel is about equal to the asymptotic communication complexity, apart from a possible additional cost that does not grow more than the logarithm of the asymptotic communication complexity. The asymptotic communication complexity of a quantum channel is obtained in the limit $S, M \to \infty$ with the sets $\mathbf{S}$ and $\mathbf{M}$ densely covering the space of quantum states and measurements, respectively.

To illustrate these results, we have evaluated the communication complexity of the following game $\mathbf{G}$. Let us denote by $\vec{v}_x$ the tridimensional vectorial function $\left(\cos\frac{\pi x}{M}, \sin\frac{\pi x}{M}, 0\right)$, where x is a real number. The measurements are projections in a two-dimensional Hilbert space. The eigenvectors of the m-th measurement in $\mathbf{M}$ correspond to the Bloch vectors $\pm\vec{v}_m$ with $m = 1, \dots, M$ and outcomes $w = \pm 1$. The set $\mathbf{S}$ contains all the $2M$ eigenvectors, that is, $\vec{v}_s$ with $s = 1, \dots, 2M$. The quantum probability of getting w given s and m is

$$P_Q(w|s, m) = \frac{1}{2}\left\{1 + w\cos\left[\frac{\pi}{M}(s - m)\right]\right\}. \quad (16)$$

We have evaluated algebraically the asymptotic communication complexity up to $M = 4$. The distributions

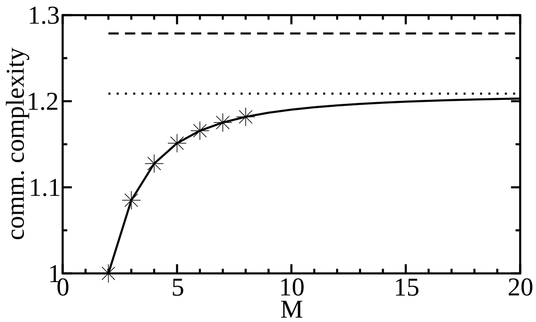

FIG. 1: Asymptotic communication complexity for $M = 2, \ldots, 20$ measurements (the solid line interpolates the data as a guide of eyes). The dot line represents the asymptotic limit of the function for $M \to \infty$. The dashed line is the communication cost of the model in Ref. [3], working for any projective measurement on the qubit. The stars are the values numerically tested.

$\rho(\mathbf{w}|s) \in \mathcal{V}(\mathbf{G})$ with minimal capacity for $M = 2, 3, 4$ are summarized by the analytical equation

$$\rho(\mathbf{w}|s) = \sum_{k=1}^{2M} P(\mathbf{w}|k)\rho(k|s) \tag{17}$$

with

$$\rho(k|s) = \sin\left(\frac{\pi}{2M}\right) \vec{v}_{k+p/2} \cdot \vec{v}_s \theta\left(\vec{v}_{k+p/2} \cdot \vec{v}_s\right), \tag{18}$$

$$P(\mathbf{w}|k) = \prod_{m=1}^{M} \theta\left(w_m \vec{v}_m \cdot \vec{v}_{k+p/2}\right), \tag{19}$$

where $p = 0$ (1) if M is odd (even) and θ is the Heaviside function. It is easy to prove that $\rho(\mathbf{w}|s)$ is an element of $\mathcal{V}(\mathbf{G})$ for any $M \geq 2$.

Since $P(\mathbf{w}|k)$ is a noiseless channel, the capacity of $\rho(\mathbf{w}|s)$ is equal to the capacity of $\rho(k|s)$. Thus, we find that the asymptotic communication complexity is

$$\mathcal{C}_{min}^{asym}(\mathbf{G}) = \mathcal{N} \sum_{n=\frac{1-M}{2}}^{\frac{M-1}{2}} \cos\left(\frac{\pi n}{M}\right) \log\left[2M\mathcal{N}\cos\left(\frac{\pi n}{M}\right)\right], \tag{20}$$

where $\mathcal{N} = \sin\left(\frac{\pi}{2M}\right)$. Note that the sum index n is not an integer when M is even. We have numerically verified the validity of Eq. (20) for M up to 8 (see Fig. 1). By symmetry, the distribution $\rho(s)$ in Eq. (7) is taken uniform. Thus the minimax problem is reduced to a minimization problem.

If we extrapolate this equation to arbitrary M, we have $\lim_{M\to\infty} \mathcal{C}_{min}^{asym}(\mathbf{G}) = 1 + \log_2 \frac{\pi}{e} \simeq 1.2088$. This value is the asymptotic communication complexity of a noiseless quantum channel with the constraint that the quantum states and the eigenstates of the measurements correspond to Bloch vectors lying on a plane. In Ref. [3], we found a protocol for any quantum state and projective measurements with communication cost equal to $\log_2(4/\sqrt{e}) \simeq 1.2786$, which is about 6% higher. It is likely that this value is actually the asymptotic communication complexity of the quantum channel for general projective measurements.

In conclusion, we have presented a general procedure for evaluating the communication complexity of channels in any general probabilistic theory, in particular quantum theory. This procedure, which relies on the reverse Shannon theorem and a strategy introduced in Refs. [3, 6], is constructive and provides a method to derive the most efficient protocol that classically simulates a channel. More explicitly, given a quantum channel, we have defined a set $\mathcal{V}$ of classical channels and proved that the minimal classical capacity in $\mathcal{V}$ is the asymptotic communication complexity of the quantum channel. Thus, the problem of evaluating the communication complexity is reduced to a minimax problem. Using the reverse Shannon theorem, the channel in $\mathcal{V}$ with minimal capacity can be turned into the most efficient classical protocol for simulating the quantum channel. We have illustrated this procedure by evaluating the asymptotic communication complexity of a noiseless quantum channel with capacity 1 qubit and some finite sets of quantum states and measurements. The procedure is numerically very stable, but the computational time of the minimax routine can grow exponentially with the number of quantum states and measurements. Thus, specific strategies reducing the computational complexity need to be devised in the case of a high number of states and measurements.

Acknowledgments. This work is supported by the Swiss National Science Foundation, the NCCR QSIT, and the COST action on Fundamental Problems in Quantum Physics. A. M. acknowledges a support in part from Perimeter Institute for Theoretical Physics, where a sketch of the proof of Theorem 1 was conceived. Research at Perimeter Institute for Theoretical Physics is supported in part by the Government of Canada through NSERC and by the Province of Ontario through MRI.

[1] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).
[2] B. F. Toner and D. Bacon, Phys. Rev. Lett. **91**, 187904 (2003).
[3] A. Montina, Phys. Rev. Lett. **109**, 110501 (2012).
[4] A. Montina, Phys. Rev. A **84**, 060303(R) (2011).
[5] C. H. Bennett, P. Shor, J. Smolin, and A. V. Thapliyal,
[6] A. Montina, arXiv:1301.3452.
[7] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991). IEEE Trans. Inf. Theory **48**, 2637 (2002).
[8] P. Harsha, R. Jain, D. McAllester, J. Radhakrishnan, IEEE Trans. Inf. Theory **56**, 438 (2010).